PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/12, 19/00

A1

(11) International Publication Number: **WO 98/27519**

(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/GB97/03448

(22) International Filing Date: 12 December 1997 (12.12.97)

(30) Priority Data:
9626020.3 14 December 1996 (14.12.96) GB

(71)(72) Applicant and Inventor: RAJA, Yogendra, Khimji [GB/GB]; 17 Baysdale Avenue, Bolton BL3 4XP (GB).

(74) Agents: GODDARD, David, John et al.; Harrison Goddard Foote, Vine House, 22 Hollins Lane, Marple Bridge, Stockport SK6 5BB (GB).

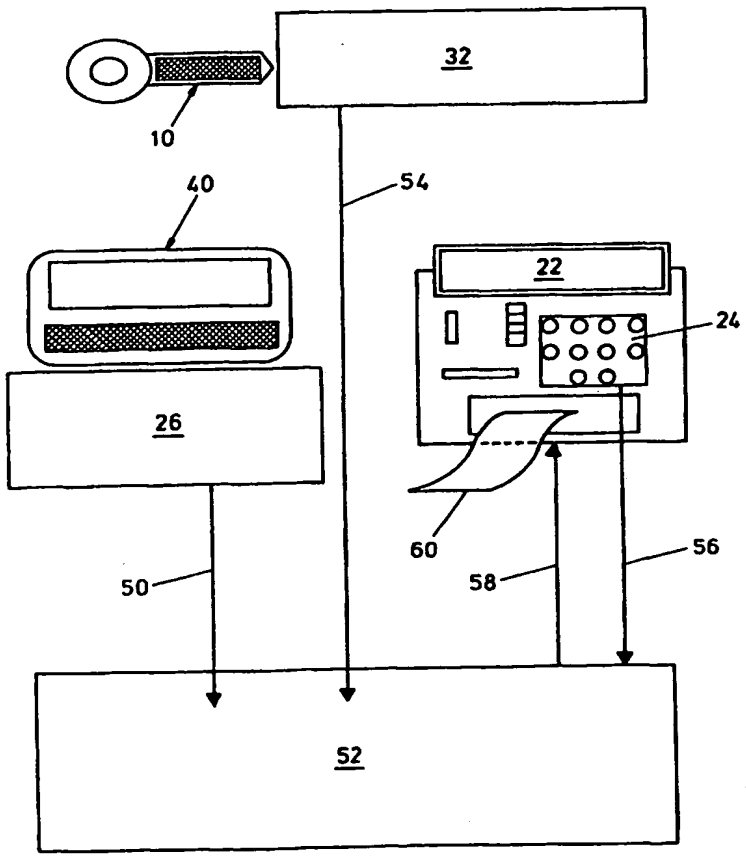
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: IMPROVEMENTS IN OR RELATING TO CREDIT CARDS

(57) Abstract

To improve security and prevent fraudulent use of a credit card (40), there is provided a verification device (10) which is separate from the credit card and bears different data, e.g. on a magnetic strip. At the time of a transaction the data is read (32) to verify that it relates to the credit card in use before the transaction is allowed to proceed. The data is preferably read by a separate reader (24) so that it never needs to leave the hands of the owner, although a common reader could be used. A PIN number may also be entered (24) at the time of the transaction for verification. Preferably the different data comprises (a) data enabling an initial verification check at the reader; (b) data which is essentially unique to a particular card for a second verification at a central computer; and (c) variable data for verification at the central computer, and which is thereafter altered and rewritten both at the central computer and on the verification device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

IMPROVEMENTS IN OR RELATING TO CREDIT CARDS.

The present invention relates to credit cards and in particular to a means and method for improving security with regard to credit cards and to preventing fraudulent use of stolen or bogus credit cards.

The term "credit card" is intended to apply to any encoded card which is used to obtain money from cash dispensers or goods or services from suppliers and retailers.

Credit cards commonly have a code magnetically encoded thereon. The code is read by a cash dispensing machine for example, the code also being supplemented by a so-called PIN (personal identification number) number which is also entered in the machine to obtain cash. In theory, only the person to whom the card is issued knows the PIN number, and therefore, only that person can obtain cash from the machine. However, thieves steal cards and have ways of discovering the PIN numbers of stolen cards such that stealing money is relatively easy.

Furthermore, a PIN number, being of necessity relatively short so it can be remembered, does not uniquely identify any single person having a credit card.

Stolen or bogus credit cards are also used to obtain goods and services from suppliers and retailers. The only means of checking whether the person is entitled to use the card is to attempt to correlate the signature on the

transaction document with that on the credit card. However, it is almost impossible to verify if a signature is genuine or not as many criminals are skilled in forging signatures.

In addition to stolen cards, it is now possible for criminals to make multiple copies of stolen cards or to manufacture fake or bogus cards which are sufficiently convincing to defraud retailers.

Levels of credit card related fraud will continue to grow because it often not possible to identify stolen cards until it is too late and it is also very difficult or impossible to identify the people who use the cards fraudulently. Currently, in the United Kingdom some 5000 cards are reported as stolen every day.

It is an object of the present invention to reduce the amount of credit card related fraud.

In a first aspect, the present invention provides credit card verification apparatus comprising a reader for reading first data encoded on a credit card, means for reading second data encoded on a credit card verification device physically separate from the credit card, wherein for any individual credit card and its associated verification device the first data is unique thereto and the second data is essentially unique thereto and different from said first data, and verification means for verifying that the first and second data relate to the same credit card.

As used herein, "essentially unique" means that the number of variations in the second data is sufficiently large that there is an insignificant chance, for example less than 10^{-6}, and preferably less than 10^{-8}, of two credit cards being associated with the same second data, even if the second data is randomly selected. Use of the uniqueness of the first data to generate the second data is possible, but if there is an algorithm connecting the first and second data, it should be selected, in known manner, so that the one is not readily derivable from the other and vice versa. However, no algorithm is necessary, it merely be required that the first data is uniquely, and the second data essentially uniquely, associated with their particular credit card account in a databank.

Where a PIN number is allocated to the credit card in question the apparatus may also comprise PIN number entry means for entering a PIN number, and the verification means may additionally determine that the PIN number so entered is that allocated to the credit card.

In a second aspect the present invention provides a method of preventing credit card fraud comprising supplying with a credit card which contains information including first encoded data, a credit card verification device which is physically separate from the credit card and contains information including second encoded data, said first data being unique to an individual credit card, and said second data being essentially unique to an individual credit card and different from said first

data, receiving first data from a credit card and second data from a verification device and acting upon said first data only when it has been determined that the first and second data relate to the same card.

The information on the credit card may include an indication that the second data, and, if appropriate, a PIN number, is required.

Again, where a PIN number has also been allocated to an individual credit card, the method may additionally include receiving a PIN number and acting upon said first data only when it has been determined that the PIN number is that allocated to the credit card.

In this specification the term "specified credit card" or "individual credit card" is meant to refer to a particular credit card or set of cards all relating to the same credit card account, issued to an individual user or group of individual users for their use only, use by others being defined herein as fraudulent use.

The verification device has its own encoded information (second data) which bears an essentially unique relation to its associated credit card, to allow use of the latter in the manner described hereinbelow. Optionally, it includes additional information relating to the person issued with the credit card, for further verification purposes by a third party.

Because it does not need to be remembered, the second data can be long or have a complicated format, unlike a PIN number. Both of these measures increase validity of verification and security.

In a preferred embodiment, verification is effected in at least two stages, and the information on the verification device comprises the second data and third data. For example, in a first verification stage, the first data and third data may be checked at the device reader itself, and only if the outcome is positive are the first data and the second data forwarded to a central computer for a second verification stage.

In such an arrangement, the third data may have a relatively simple relation to the first data, for example it may be the same as the first data, or be derivable therefrom by a relatively simple algorithm. The third data is preferably unique or essentially unique to an individual credit card, but need not be so. Nevertheless, the second data is unique, or essentially unique to the credit card, and so provides a greater degree of security.

Even more preferably, where the information recorded on the verification device is re-writable, the device may include variable fourth data. In use, the fourth data is also sent to the central computer for verification that it relates to the credit card, and once verification has taken place, the fourth data is altered according to any known algorithm, including the selection of a random

number, recorded at the central computer, and re-written to replace the existing fourth data on the verification device.

In this manner, even if the information on a verification device and on a credit card is copied by a fraudster, provided the true owner uses the card before the fraudster, the latter will be prohibited from using the card, because the fourth information will have been altered in the meantime. It is true that should the fraudster manage to use the card before the true owner, then the latter will be unable to use the card, but this may be considered to be advantageous. Since the true owner may well be unaware that the information on the card and device have been copied ((and, if appropriate, the PIN number known), so that cash is being drained from the related account, the inability to use the card will (or should) provide an alert to the owner, or the credit card company when the owner complains or the system detects an apparently fraudulent attempt to use the card, that fraudulent use of the card may have taken place, thus enabling checks to be made and the extent of the fraud to be reduced.

Clearly, data similar to the third and fourth data could also be provided on the credit card itself. In particular, variable fourth data on the credit card could also prove useful in reducing the extent of fraud in transactions using credit cards without the associated verification device.

Preferably none of the second, third and fourth data is identical to a PIN number associated with the credit card, or identical to data provided by the card itself, although it would be possible for the second data to equate thereto in a relatively low security arrangement.

The use of the variable fourth variable data itself provides an enhanced degree of security. Thus, in a third aspect the invention provides credit card verification apparatus comprising a reader for reading first data encoded on a credit card, means for reading and writing variable data encoded on a credit card verification device physically separate from the credit card, said variable data being different from said first data, verification means including a data store for verifying that the first and variable data as read relate to the same credit card, and upon said verification being positive, altering said variable data, storing said altered variable data in said data store, and replacing said variable data with said altered variable data on said verification device.

Correspondingly, in a fourth aspect the invention provides a method of preventing credit card fraud comprising supplying with a credit card which contains information including first encoded data, a credit card verification device which is physically separate from the credit card and contains information including encoded variable data different from said first data, receiving first data from a credit card and said variable data from a verification device and acting upon said first data

only when it has been determined that the first and variable data relate to the same card, said acting upon including the step of subsequently altering said variable data on the verification device and storing the altered variable data for use when repeating the said method.

It will be clear that the invention in its third and fourth aspects can be combined with the invention in its first and second aspects respectively. Thus, for example, the verification device may also contain the second and/or third data for use as described herein in relation to the invention in its first and second aspects.

The information on the verification device may be encoded in any known suitable form such as by means of a magnetically encoded strip, optical encoding (preferably invisible to the human eye), an rf transponder, a microchip or any other form of readable information retaining means.

Clearly, it is advisable for the owner to keep the credit card and the verification device separate, just as it is recommended that any document recording a PIN number should be kept separately (and preferably not indicating that it contains information regarding the PIN number). While the verification device could be in the form of another card, there then exists a strong temptation to place them both in the same location, for example in the same wallet or purse, particularly if it is of the same size and shape as the credit card.

Preferably, therefore, the verification device is given an different shape and/or size reducing this temptation. In a particularly preferred form, the verification device is in the form of a key, having an apertured handle portion enabling it to be attached to a key-ring.

Thus, in a fifth aspect, the invention provides a credit card verification device having a flat or three-dimensional shape of a key, and bearing thereon machine readable information.

The key need only be as large as is necessary to enable information thereon to be read by an appropriate reader. The key may be of metal, providing this does not interfere with the reading of the information thereon (this will depend on how the information is recorded), but could be of an alternative material such as plastics or card. Preferably, the key shape is three-dimensional - for example with significant thickness, and preferably a non-uniform thickness, such as a cylindrical shank and flat apertured handle.

UK Patent Application No. 2 181 582 (Blackwell) discloses an electronic device, such as in the form of a watch, which is provided with a secure store for personal identity information, such information being available for use either on a display (e.g. of the watch) for transmission to equipment to which access is sought. It is mentioned that this device could be used to display or transmit coded information for use in conjunction with

information on a credit card and a PIN number to provide additional security. It is believed that the PIN number referred to here is that (a personal number) used for gaining access to information held in the device (this information could be for example a conventional PIN number associated with a credit card) rather than the conventional PIN number itself. In such a case this device merely constitutes a new way of retrieving a conventional PIN number when a credit card is used, and as noted above, PIN numbers are not generally unique to individual cards. This method possibly provides greater security insofar as access to the PIN number itself requires input of a personal number into the device, but is not considered to provide the degree of security afforded by the present invention.

Furthermore, the device is an active electronic device requiring a power source such as a battery, means for entering and storing the personal identity information, and means for retrieving and transmitting or displaying such information, all within the device itself. Thus the device is relatively complicated, and becomes useless if the battery fails.

In a preferred form of the present invention, the information is held by passive readable means for active reading by an external reader - thus, as later described in relation to a preferred embodiment, it would sufficient simply to write information on a magnetic strip at the time of producing the verification device, and to read the second and/or other data therefrom by an

external reader at the point of use. There is no PIN number necessary for accessing the information on the verification device, rather such information is obtained and is correlated with information from the credit card and/or associated PIN number for verification purposes, any known coding method of the various items of information being employed, preferably such as provides a high degree of security, as mentioned above and later.

The specified credit card and its associated verification device are unique to one another. However, where a card issuer issues more than one credit card of one account holder to a group of people such as, for example, other members of the account holder's family such as the wife or husband, each verification device associated with an individual card could be identical or different. Where there is variable fourth information on the verification device, as mentioned previously, then it will be necessary for each verification device to differ, so as to be identifiable and capable of being associated with its own variable information, to prevent the use of a card by one of the said group prohibiting use by other member of the group. However, even in these circumstances the encoded information on the credit card is usually the same as it frequently relates to an individual account holder's details. In these circumstances, for example, there would be issued one verification device for each issued individual credit card.

In use the specified credit card would be issued to a person or group of persons by the card issuer together with a separate verification device by any known means. Usual security precautions may apply such that the account is only activated when the recipient of the cards acknowledges safe receipt for example. The credit card and the verification device would be kept by the person separate from each other, the verification device perhaps being kept on a key-ring with other keys for example.

To effect a transaction at a cash dispenser for example by the present invention, the credit card would be inserted in the machine in known manner and the user's PIN number entered, the person then also being required to insert his verification device in the machine. A database to which the machine is connected and which holds details of the person's account then verifies that the correct corresponding details between the information encoded on the credit card, PIN number and information encoded on the verification device meet predetermined criteria before issuing cash to the person. Thus, if the credit card per se is stolen and even if the thief knows the person's PIN number it will not be possible for him to withdraw cash without the verification device.

Similarly, when a person is securing goods or services at a shop for example, it will be necessary for the person to provide his verification device. In addition to the credit card being "swiped" or inserted into a means of reading the encoded information thereon, the verification device will also be swiped or otherwise read. In the

absence of the verification device, the transaction will not occur in case the credit card has been stolen. Thus, in addition to the usual signature from the person receiving the goods or services, the retailer will also have the assurance of the credit card being verified by the verification device; the transaction not proceeding unless the information on the credit card and verification device meet the predefined criteria held in the database. Preferably, the verification device will always remain with the user and will not be taken by a retailer together with the credit card into another room for example to be swiped. Thus, there should always be a means of reading the verification device at a convenient location such that the verification device always remains within sight of the user.

It will be apparent to those skilled in the computer and information technology art that many different forms of hardware means and software means may be provided to support the method and article of the present invention. For example, the order in which the credit card PIN number and verification device are entered into the information reading means may be any that correspond to or are dictated by the particular software.

Similarly, software may be produced whereby the credit card and verification device be entered sequentially in the same receiver in the information reading means. In this embodiment, existing hardware may be retained and only the software changed.

With the method of the present invention it may not be necessary for there to be a PIN number, which can easily be forgotten by a user, the credit card and verification device together being sufficient. However, in the interests of security, it is preferable that the present invention be used in conjunction with a conventional PIN number.

In a particularly preferred form, verification is done in two stages. First verification means, for example in the card reader itself, performs a check on information provided by the card or verification device or both (for example, a simple parity check to verify that the coded information is of acceptable form and valid per se, but preferably, as mentioned above, a check on the third data to establish that it relates to the credit card), and second verification means, for example in a host computer receiving output from the reader, performs a further check on both sets of information (preferably, as mentioned above, verification that the second and variable fourth data relate to the credit card and the present state of the verification device respectively). In known manner, failure to achieve verification can be arranged to cause non-return of the credit card and/or verification device. It will be clear that this mode of operation can be practised with the additional input of a PIN number.

The verification device could also contain encoded information relating for example to the appearance and gender of the person using it, or to a car registration

or NHS number, enabling the retailer who suspects fraud to verify visually or by interrogation that the person using it corresponds to such information.

In order that the present invention may be more fully understood, an example of the present invention will now be described by way of illustration only with reference to the accompanying drawings, of which:

Figure 1 shows a schematic view of a verification device having a key-shape according to the present invention, for use in the verification apparatus and method of the invention;

Figure 2 shows a schematic view of a cash dispenser for use with the present invention;

Figure 3 shows a schematic of a credit card; and,

Figure 4 which shows a block diagram illustrating the method of the present invention.

Referring now to the drawings and where the same features are denoted by common reference numerals.

Figure 1 shows a verification device 10 according to the present invention, henceforth referred to briefly as a "cardkey". The cardkey is in the shape of a key and made of a stiff, durable plastics material and intended to be kept by a user on a key-ring (not shown) by the head 12. The cardkey 10 has information encoded on a magnetic

strip 14 affixed to the shank 16 of the cardkey. In modifications (a) the cardkey is made of metal; (b) the card key has a three dimensional key shape; and/or (c) the coding is other than magnetic, e.g. optical.

Figure 2 shows a schematic view in elevation of a cash dispensing machine 20. The machine 20 has the usual features to be found in such devices including; a display screen 22 for imparting instructions and/or information to the user; a keypad 24 for entering numbers; a slot 26 for receiving a credit card; a keypad 28 for answering standard questions made by the device 20; a cash dispenser slot 30; and, a slot 32 for receiving the cardkey 10.

Figure 3 shows a schematic view of a conventional plastics material credit card 40 which has a standard rectangular body 42 having the usual embossed information relating to the person to whom it is issued, expiry date, account number and so forth and a magnetic strip 44 having information encoded thereon.

Figure 4 shows a block diagram indicating the cardkey 10, cash dispenser 20, credit card 40 and a central database 52. The cardkey contains second, third and fourth data as described previously, neither of the second and fourth data equating to information on the credit card itself. The third data can, but need not, correspond to information on the credit card for a preliminary check at the reading stage.

The credit card 40 is entered in the slot 26 of the machine 20 and the information thereon is read 50 in known manner and verified against data held in the central data base 52; an invitation is issued to enter the cardkey in the slot 32 of the machine 20 and at least the third data is read 54 by known means.

Either in the in the central database 52 or the reader, but preferably the latter in cases where the first and third data have a predetermined relation, the third data is verified by correlation with the first data. The reader then reads the second and fourth data, if it has not done so when determining the third data, for transmission to the central database and correlation with stored information relating to the credit card and verification device. Meanwhile, the user's PIN number is entered on the keypad 24 which again is verified 56 by the database 52. Only when all verifications have been satisfactorily completed does the database 52 enable 58 the machine 20 to issue the cash 60 requested by the user. At this stage the fourth data is altered, the altered data is stored at the central database, and also written over the existing fourth data on the cardkey.

In an alternative embodiment the slot 32 for the card key 10 may also be the same as the slot 26 for the credit card 40, the cardkey 10 being in a similar physical form to the card 40. In this embodiment, the credit card 40, PIN number and cardkey 10 are entered sequentially into the machine 20 in response to instructions displayed in the window 22 of the machine 20.

It will be apparent to those skilled in the art that all of the hardware means to put the present invention into effect are already known in the art. The present invention once known to a person skilled in the computer software art may be put into effect by the writing of appropriate enabling software.

CLAIMS

1. Credit card verification apparatus comprising a reader for reading first data encoded on a credit card, means for reading second data encoded on a credit card verification device physically separate from the credit card, wherein for any individual credit card and its associated verification device the first data is unique thereto and the second data is essentially unique thereto and different from said first data, and verification means for verifying that the first and second data relate to the same credit card.

2. Credit card verification apparatus according to claim 1 and further comprising PIN number entry means for entering a PIN number, and verification means for establishing that the PIN number is associated with the credit card.

3. Apparatus according to claim 1 or claim 2 wherein the second data is magnetically or optically encoded.

4. Apparatus according to any preceding claim wherein the first and second reading means are the same means.

5. Apparatus according to any one of claims 1 to 3 wherein the first and second reading means are different means.

6. Apparatus according to any preceding claim wherein the PIN number entry means is a keyboard for manual input.

7. A method of preventing credit card fraud comprising supplying with a credit card which contains information including first encoded data, a credit card verification device which is physically separate from the credit card and contains information including second encoded data, said first data being unique to an individual credit card, and said second data being essentially unique to an individual credit card and different from said first data, receiving first data from a credit card and second data from a verification device and acting upon said first data only when it has been determined that the first and second data relate to the same card.

8. A method according to claim 7 wherein a PIN number is also associated with the credit card, and said acting upon said first data is conditional upon receipt of said PIN number.

9. A method according to claim 7 or claim 8 wherein the information on the credit card is indicative of the fact that the second data is required.

10. A method according to any one of claims 7 to 9 wherein the verification device comprises third data for verification by correlation with said first data before said acting is enabled.

11. A method according to any one of claims 7 to 10 wherein the verification device comprises fourth data, said acting is enabled only when it has been verified that the fourth data relates to the said credit card, and wherein said fourth data is subsequently altered, the altered fourth data being written on the verification device in place of the existing fourth data, and also being stored in association with other information identifying the credit card, for verification purposes upon a later use of the verification device.

12. A method according to any one of claims 7 to 11 wherein the verification device has a two or three dimensional shape of a key.

13. Credit card verification apparatus comprising a reader for reading first data encoded on a credit card, means for reading and writing variable data encoded on a credit card verification device physically separate from the credit card, said variable data being different from said first data, verification means including a data store for verifying that the first and variable data as read relate to the same credit card, and upon said verification being positive, altering said variable data, storing said altered variable data in said data store, and replacing said variable data with said altered variable data on said verification device.

14. A method of preventing credit card fraud comprising supplying with a credit card which contains information including first encoded data, a credit card verification

device which is physically separate from the credit card and contains information including second encoded variable data different from said first data, receiving first data from a credit card and variable data from a verification device and acting upon said first data only when it has been determined that the first and variable data relate to the same card, said acting upon including the step of subsequently altering said variable data on the verification device and storing the altered variable data for use when repeating the said method.

15. A credit card device having a flat or three-dimensional shape of a key, and bearing thereon machine readable information.

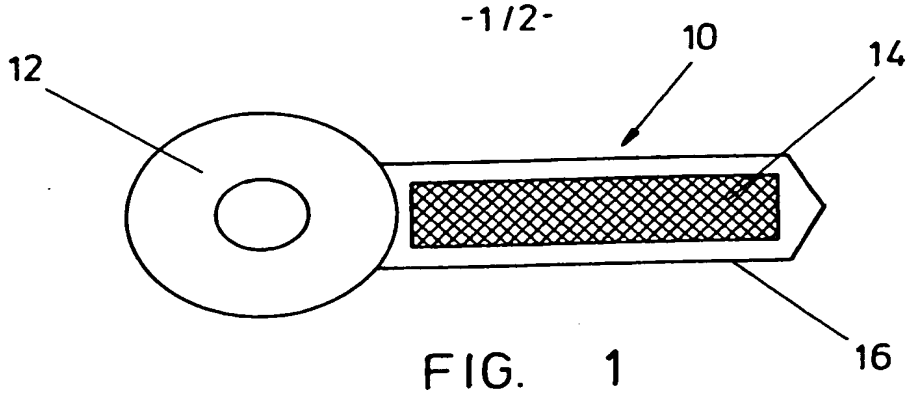


FIG. 1

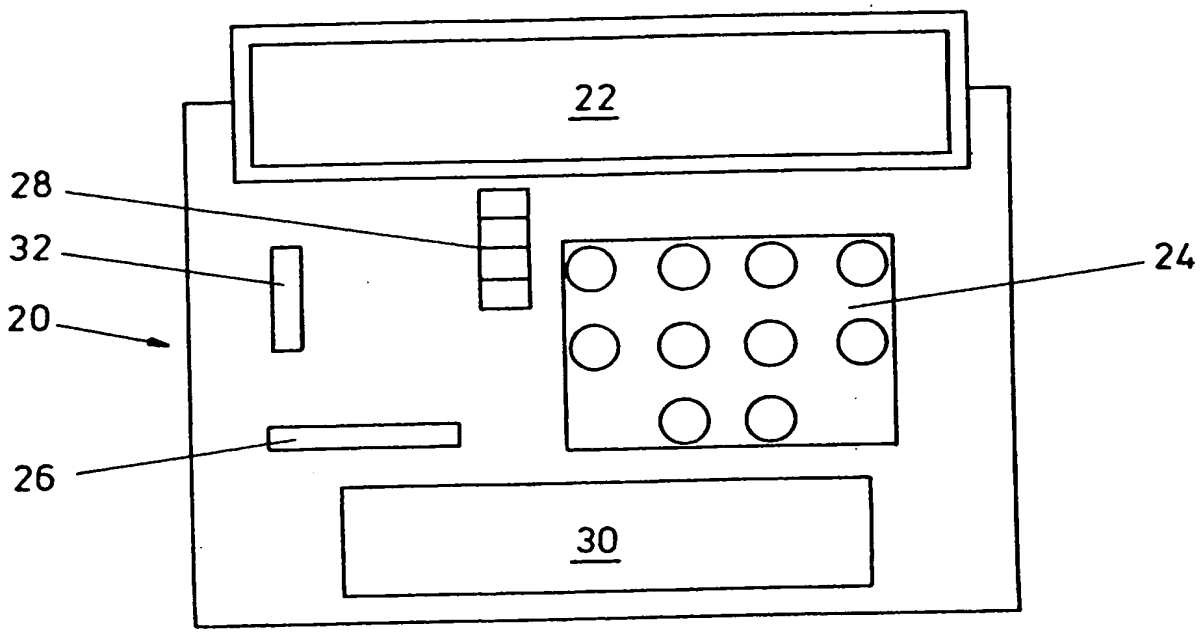


FIG. 2

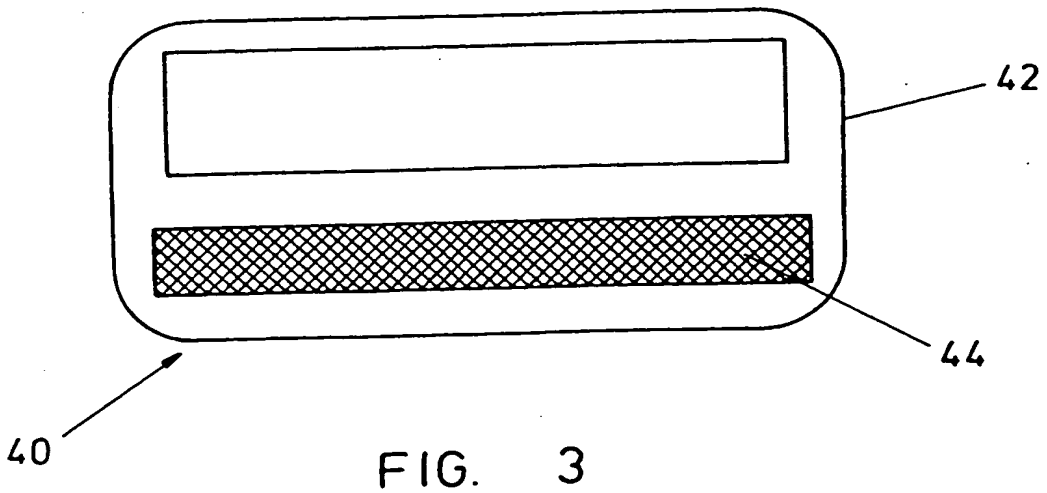


FIG. 3

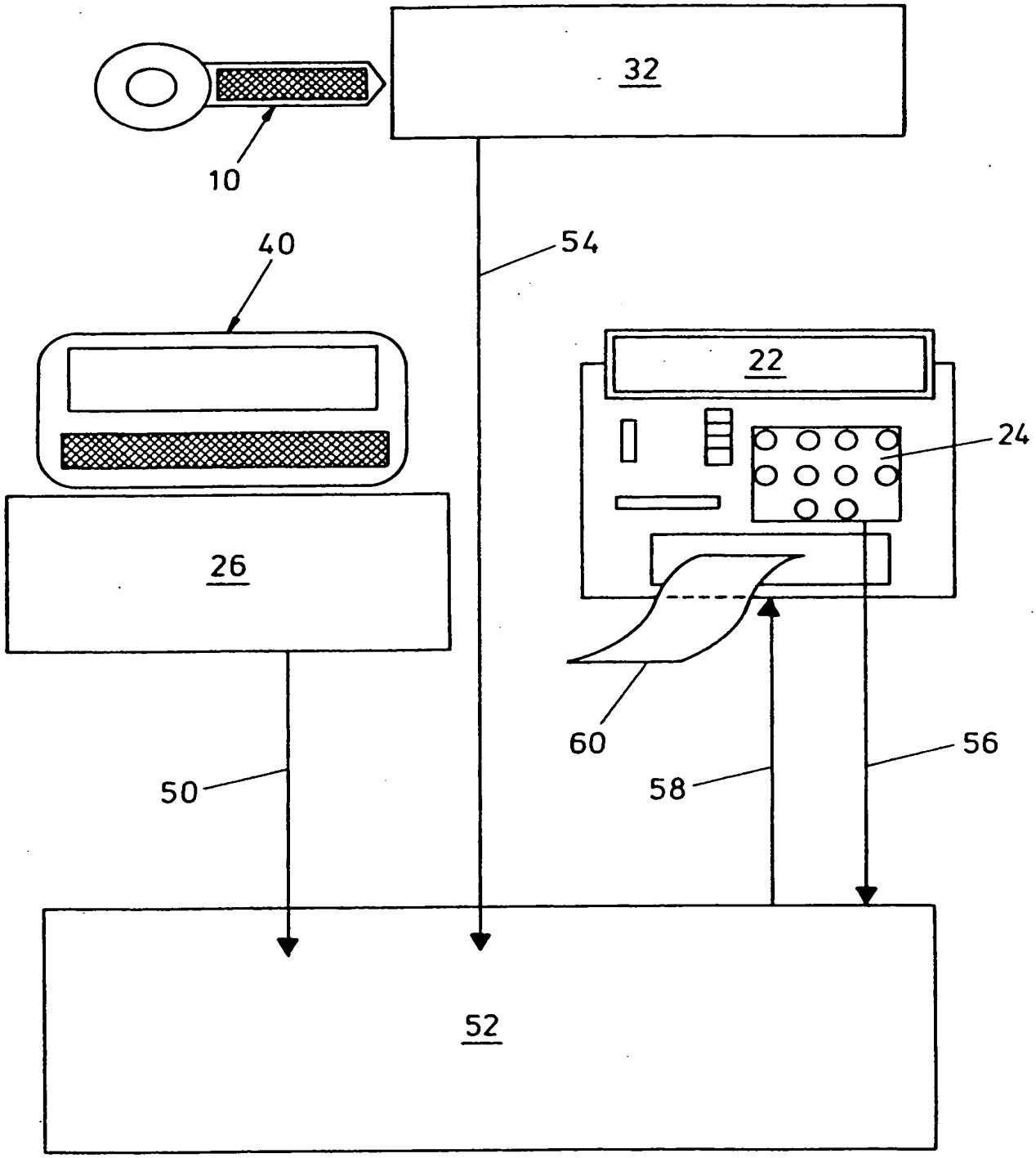


FIG. 4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 97/03448

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/12 G07F19/00

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 3 593 291 A (G.S. CARTER) 13 July 1971	1,5,7, 12,15
A	see abstract; claims; figures 1,2	13,14
A	EP 0 106 361 A (OMRON TATEISI ELECTRONICS) 25 April 1984 see abstract; claims; figures	1-4,6-8, 10,12-15
A	EP 0 397 512 A (MATERIAL ENGINEERING TECHNOLOGY LABORATORY) 14 November 1990 see abstract; claims; figures 1-3 see column 2, line 38 - column 4, line 31	1-15
A	US 3 859 508 A (J. BROSOW) 7 January 1975	
A	US 3 582 890 A (L.C. RIVERS) 1 June 1971	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 May 1998	20/05/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 97/03448

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 552 078 A (GEMPLUS CARD INTERNATIONAL) 21 July 1993	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 97/03448

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 3593291 A	13-07-1971	NONE	
EP 0106361 A	25-04-1984	JP 1675826 C	26-06-1992
		JP 3041865 B	25-06-1991
		JP 59072572 A	24-04-1984
		DE 3382475 A	23-01-1992
		US 4562340 A	31-12-1985
EP 0397512 A	14-11-1990	JP 2297297 A	07-12-1990
US 3859508 A	07-01-1975	SE 384940 B	24-05-1976
		DE 2318263 A	25-07-1974
US 3582890 A	01-06-1971	NONE	
EP 0552078 A	21-07-1993	FR 2686172 A	16-07-1993
		DE 69309119 D	30-04-1997
		DE 69309119 T	14-08-1997
		ES 2098686 T	01-05-1997
		JP 2593836 B	26-03-1997
		JP 8022521 A	23-01-1996
		US 5486687 A	23-01-1996
		US 5375037 A	20-12-1994